# EARLY IDENTIFICATION OF CYBER THREATS BY DETECTING ANOMALIES BASED ON ARTIFICIAL INTELLIGENCE

**Bekmurodov Ulugbek Bakhrom ugli**
*Associate Professor, Samarkand Branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, PhD*
**Almardonov Asliddin Fakhriddin ugli**
*Master's student, Samarkand Branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi*
*bekmurodov1987@gmail.com*
*aslialimardonov@gmail.com*

**Abstract:** *This scientific article is devoted to the issue of early identification of cyber threats by detecting anomalies based on artificial intelligence. The complexity and dynamic nature of cyberattacks in modern information and communication systems significantly reduce the effectiveness of traditional signature-based security systems. Therefore, this study examines approaches to anomaly detection based on artificial intelligence and machine learning technologies for identifying cyber threats.*

*In the research process, unsupervised and semi-supervised machine learning methods were applied based on the analysis of normal network traffic behavior. In particular, anomaly detection mechanisms were developed using clustering algorithms and deep learning-based Autoencoder models. Network traffic data were cleaned, normalized, and used to train models primarily on normal activity patterns due to the limited availability of labeled attack data in real-world environments.*

*The obtained results demonstrate that artificial intelligence-based anomaly detection approaches enable the early identification of unknown and zero-day cyberattacks. These approaches support the transition from reactive to proactive cybersecurity mechanisms and provide a scientific foundation for integrating artificial intelligence-based anomaly detection methods into real network infrastructures.*

**Keywords:** *artificial intelligence, cybersecurity, anomaly detection, cyber threats, machine learning, network traffic, proactive protection, Autoencoder, zero-day attacks.*

## INTRODUCTION

The rapid development of digital technologies and the widespread use of information systems have made cybersecurity one of the strategic challenges of modern society. Along with the growth in the number of cyber threats, their complexity, stealth, and adaptability are also increasing. Traditional cybersecurity systems primarily rely on known attack patterns and signature-based detection methods, which impose significant limitations on identifying new or unknown attacks (Figure 1).

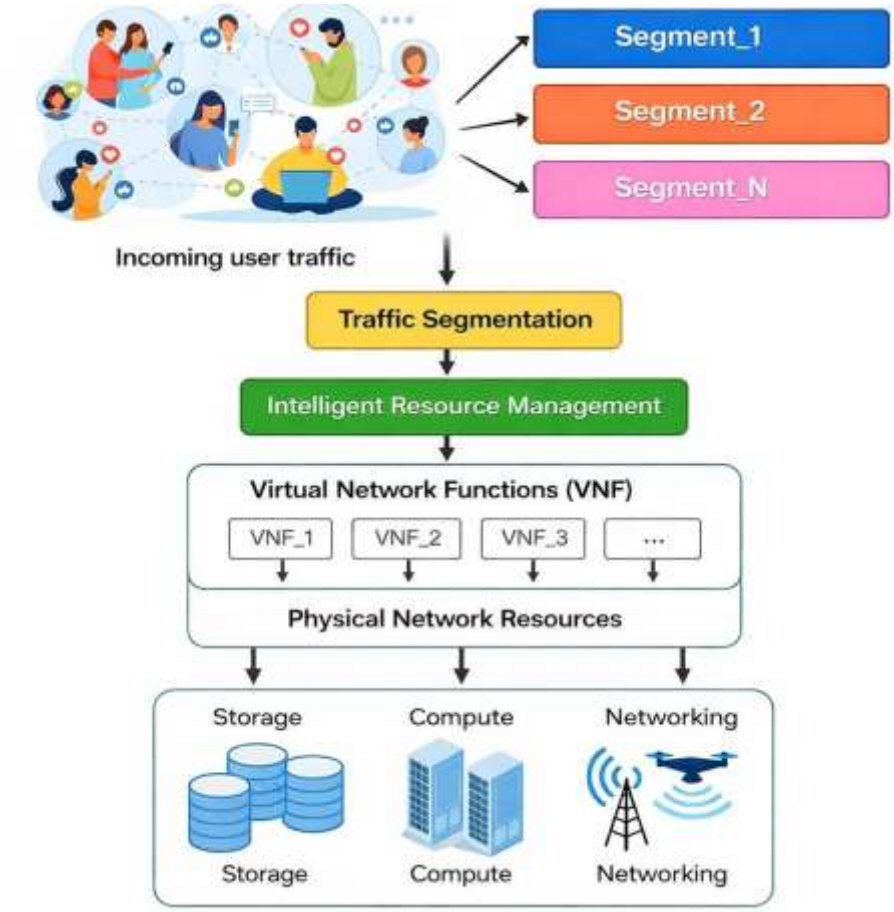


Figure 1. General architecture of network resource management based on artificial intelligence.

In recent years, artificial intelligence and machine learning technologies have gained increasing importance in addressing these challenges. In particular, anomaly detection methods enable the identification of deviations from normal system behavior by learning typical operational patterns. Such approaches are especially effective for the early identification of cyber threats whose characteristics are not known in advance.

The main objective of this study is to develop and analyze methods for early cyber threat detection through anomaly detection based on artificial intelligence and to assess their effectiveness. The main research tasks include analyzing the limitations of traditional cybersecurity approaches, studying anomaly-based machine learning models, developing anomaly detection mechanisms using network traffic data, and evaluating the effectiveness of artificial intelligence-based approaches.

The scientific novelty of this research lies in substantiating anomaly detection methods based on artificial intelligence as a proactive approach to cyber threat identification and proposing a conceptual framework suitable for modern virtualized and dynamic network environments.

2. METHODS

In this study, network traffic data were selected as the primary source of information for detecting cyber threats. Initially, the collected data were preprocessed by removing noisy and duplicate records and normalizing feature values to a uniform

range. This preprocessing stage is essential to ensure the stable and accurate operation of artificial intelligence models.

Due to the limited availability of labeled attack data in real-world environments, the models were trained mainly on data representing normal network activity. Unsupervised and semi-supervised machine learning algorithms were employed for anomaly detection. Clustering methods were used to group normal network behavior, while data points located outside these clusters were considered suspicious (Figure 1).


Figure 2. Processes of early identification of cybersecurity threats.

Additionally, a deep learning-based Autoencoder model was applied. The Autoencoder is designed to reconstruct normal data with minimal error, whereas anomalous data result in significantly higher reconstruction errors. During real-time testing, incoming network traffic was continuously monitored, and reconstruction errors or deviation levels were calculated for each data instance. If the deviation exceeded a predefined threshold, the event was identified as a potential cyber threat, and an alert was generated.

**3. RESULTS**

The experimental results indicate that artificial intelligence-based anomaly detection systems provide higher accuracy and adaptability compared to traditional signature-based security mechanisms. In particular, Autoencoder-based models demonstrated effective performance when processing large-scale and complex network traffic data.

The results also revealed that adaptive threshold selection plays a crucial role in reducing false positive detections. Properly configured models were able to detect unknown and zero-day attacks at early stages, confirming the effectiveness of anomaly-based approaches for proactive cybersecurity.

4. DISCUSSION

The main advantage of anomaly-based detection approaches lies in their ability to identify previously unseen cyber threats without relying on predefined attack

signatures. This makes them highly suitable for dynamic and evolving network environments. However, such systems require large volumes of high-quality data and significant computational resources.

Moreover, incorrect modeling of normal network behavior may lead to excessive false alerts. Therefore, integrating anomaly-based approaches with traditional signature-based systems is recommended to form a hybrid cybersecurity architecture that combines accuracy with robustness.

## 5. CONCLUSION

This study demonstrates that artificial intelligence-based anomaly detection methods enable the early identification of cyber threats and support the transition from reactive to proactive cybersecurity strategies. By analyzing deviations from normal network behavior, such systems can identify potential attacks before significant damage occurs, thereby enhancing the reliability, continuity, and stability of information systems.

The research results also highlight the importance of data quality, proper model configuration, and efficient use of computational resources when deploying anomaly detection systems in real network infrastructures. Future research should focus on developing adaptive and hybrid approaches to further improve detection accuracy and reduce false positives. Overall, artificial intelligence-based anomaly detection represents a key component of modern cybersecurity systems and provides a solid foundation for future scientific and practical advancements in this field.

## REFERENCES:

1. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy.

2. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. ACM Computing Surveys.

3. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press.

4. Patcha A., Park J. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks.

5. Lakhina A. et al. Mining Anomalies Using Traffic Feature Distributions. ACM SIGCOMM.